10/661,650

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１０月１１日

出 願 番 号
Application Number: 特願２００２－２９９６５８

[ST. 10/C]: ［ＪＰ２００２－２９９６５８］

出 願 人
Applicant(s): 株式会社リコー

２００３年 ８月２７日

特許庁長官
Commissioner,
Japan Patent Office 今 井 康 夫

出証番号 出証特２００３－３０６９７６０

【書類名】　特許願
【整理番号】　0207088
【提出日】　平成14年10月11日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/00　530
【発明の名称】　アクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体
【請求項の数】　19
【発明者】
【住所又は居所】　東京都大田区中馬込１丁目３番６号
株式会社リコー内
【氏名】　金井　洋一
【特許出願人】
【識別番号】　000006747
【氏名又は名称】　株式会社リコー
【代表者】　桜井　正光
【代理人】
【識別番号】　100084250
【弁理士】
【氏名又は名称】　丸山　隆夫
【電話番号】　03-3590-8902
【手数料の表示】
【予納台帳番号】　007250
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1

【包括委任状番号】　0207936

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　アクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体

【特許請求の範囲】

【請求項１】　所定のネットワークに接続されたアクセス制御サーバであって、

前記ネットワークを介して電子データの作成者の端末から前記電子データを受信する電子データ受信手段と、

前記受信された電子データのデータ種別を示す情報および前記受信された電子データに係るユーザのユーザＩＤを含むワークフロー情報を受信するワークフロー情報受信手段と、

電子データに対するユーザの種別ごとのアクセス権限を示すアクセス権限テンプレートを電子データのデータ種別ごとに１つ以上格納するテンプレート格納手段と、

前記格納された１つ以上のアクセス権限テンプレートから、前記受信されたワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出手段と、

前記抽出されたアクセス権限テンプレートに、各ユーザの前記ユーザＩＤを挿入して、前記受信された電子データに対する前記各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成手段と、

を有することを特徴とするアクセス制御サーバ。

【請求項２】　前記受信された電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信手段と、

前記アクセス制限情報に基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成手段と、

前記生成されたアクセス制限データを前記ネットワークを介して送信するデータ送信手段と、

を有することを特徴とする請求項１記載のアクセス制御サーバ。

【請求項３】　前記テンプレート格納手段は、

前記ユーザの種別として、前記電子データの作成者、前記電子データの承認者、および前記アクセス制限データの送信先のユーザが設定されている前記アクセス権限テンプレートを格納することを特徴とする請求項２記載のアクセス制御サーバ。

【請求項４】　前記アクセス制限データ生成手段は、

予め自サーバに格納されたセキュリティポリシーに基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする請求項２または３記載のアクセス制御サーバ。

【請求項５】　前記アクセス制限データ生成手段は、

前記受信された電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする請求項２から４のいずれか１項に記載のアクセス制御サーバ。

【請求項６】　所定のネットワークに接続され、電子データに対するアクセス制御を行うアクセス制御サーバを用いた電子データ発行ワークフロー処理方法であって、

前記アクセス制御サーバが、前記ネットワークを介して電子データの作成者の端末から前記電子データを受信する電子データ受信工程と、

前記アクセス制御サーバが、前記受信した電子データのデータ種別を示す情報および前記受信された電子データに係るユーザのユーザＩＤを含むワークフロー情報を受信するワークフロー情報受信工程と、

前記アクセス制御サーバが、電子データに対するユーザの種別ごとのアクセス権限を示すアクセス権限テンプレートを電子データのデータ種別ごとに１つ以上格納するテンプレート格納工程と、

前記アクセス制御サーバが、前記格納した１つ以上のアクセス権限テンプレートから、前記受信したワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出工程と、

前記アクセス制御サーバが、前記抽出したアクセス権限テンプレートに、各ユーザの前記ユーザＩＤを挿入して、前記受信した電子データに対する前記各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成工程

と、

を有することを特徴とする電子データ発行ワークフロー処理方法。

【請求項７】　前記アクセス制御サーバが、前記受信した電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信工程と、

前記承認情報受信後に、前記アクセス制御サーバが、前記アクセス制限情報に基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成工程と、

前記アクセス制御サーバが、前記生成されたアクセス制限データを前記ネットワークを介して送信するデータ送信工程と、

を有することを特徴とする請求項６記載の電子データ発行ワークフロー処理方法。

【請求項８】　前記アクセス制御サーバが、前記アクセス制限情報に基づいて、前記受信した電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成工程と、

前記アクセス制御サーバが、前記受信した電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信工程と、

前記アクセス制御サーバが、前記承認情報を受信すると、前記生成されたアクセス制限データを前記ネットワークを介して送信するデータ送信工程と、

を有することを特徴とする請求項６記載の電子データ発行ワークフロー処理方法。

【請求項９】　前記テンプレート格納処理は、

前記ユーザの種別として、前記電子データの作成者、前記電子データの承認者、および前記アクセス制限データの送信先のユーザが設定されている前記アクセス権限テンプレートを格納することを特徴とする請求項７または８記載の電子データ発行ワークフロー処理方法。

【請求項１０】　前記アクセス制限データ生成工程は、

前記アクセス制御サーバが、予め自サーバに格納したセキュリティポリシーに基づいて、前記受信した電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする請求項７から９のいずれか１項に記載の電子デー

タ発行ワークフロー処理方法。

【請求項１１】　前記アクセス制限データ生成工程は、

前記受信した電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする請求項７から１０のいずれか１項に記載の電子データ発行ワークフロー処理方法。

【請求項１２】　電子データの作成者により作成された前記電子データの受信制御を行う電子データ受信処理と、

前記受信された電子データのデータ種別を示す情報および前記受信された電子データに係るユーザのユーザＩＤを含むワークフロー情報の受信制御を行うワークフロー情報受信処理と、

電子データに対するユーザの種別ごとのアクセス権限を示す１つ以上のアクセス権限テンプレートを電子データのデータ種別ごとに格納するテンプレート格納処理と、

前記格納された１つ以上のアクセス権限テンプレートから、前記受信されたワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出処理と、

前記抽出されたアクセス権限テンプレートに、各ユーザの前記ユーザＩＤを挿入して、前記受信された電子データに対する前記各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成処理と、

をコンピュータに実行させるためのプログラム。

【請求項１３】　前記受信された電子データの発行が承認者により承認された旨の承認情報の受信制御を行う承認情報受信処理と、

前記承認情報受信後に、前記アクセス制限情報に基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成処理と、

前記生成されたアクセス制限データの送信制御を行うデータ送信処理と、

をコンピュータに実行させるための請求項１２記載のプログラム。

【請求項１４】　前記アクセス制限情報に基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限デー

タ生成処理と、

前記受信された電子データの発行が承認者により承認された旨の承認情報の受信制御を行う承認情報受信処理と、

前記承認情報の受信を認識すると、前記生成されたアクセス制限データの送信制御を行うデータ送信処理と、

をコンピュータに実行させるための請求項１２記載のプログラム。

【請求項１５】　前記テンプレート格納処理は、

前記ユーザの種別として、前記電子データの作成者、前記電子データの承認者、および前記アクセス制限データの送信先のユーザが設定されている前記アクセス権限テンプレートを格納することを特徴とする請求項１３または１４記載のプログラム。

【請求項１６】　前記アクセス制限データ生成処理は、

セキュリティポリシーに基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする請求項１３から１５のいずれか１項に記載のプログラム。

【請求項１７】　前記アクセス制限データ生成処理は、

前記受信された電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする請求項１３から１６のいずれか１項に記載のプログラム。

【請求項１８】　請求項１２から１７のいずれか１項に記載のプログラムを実行するコンピュータ装置。

【請求項１９】　請求項１２から１７のいずれか１項に記載のプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、アクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体に関し、特に、ファイルの作成者により指定されたファイルの種類、ファイルの承認者および配布先などに基づ

いて、作成したファイルに対するアクセス権限の制御を行うアクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体に関する。

【０００２】

【従来の技術】

従来、ネットワーク上の電子データに対する各ユーザの利用権限が記録されたアクセスコントロールリスト（Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ｌｉｓｔ：ＡＣＬ）に基づいて、発行したファイルのアクセス制御を行っていた。ＡＣＬを用いて電子データに対するアクセス制御を行う従来技術として、特開２００１－１４２８７４号公報（以下、特許文献１）が開示するところの文書管理システム、および特開２００１－１９５２９５号公報（以下、特許文献２）が開示するところの統合型技術文書管理装置があった。

【０００３】

特許文献１および引用文献２では、文書を作成して登録し、承認されると文書を印刷可能なＰＤＦ（登録商標）ファイルと印刷不可能なＰＤＦファイルに変換し、利用権限に応じて、閲覧できるファイルを制限していた。

【０００４】

【特許文献１】

特開２００１－１４２８７４号公報

【特許文献２】

特開２００１－１９５２９５号公報

【０００５】

【発明が解決しようとする課題】

しかしながら、従来の技術では、電子データによるファイルを作成する度に、ユーザごとにファイルの利用権限を示す情報を入力する必要があり、多数のユーザがそのファイルを利用する場合、利用権限を示すデータを生成するために多大な労力および時間を費やさなければならなかった。

【０００６】

本発明は、上記問題点に鑑みてなされたものであり、電子データに対する利用

権限を示すデータ（ＡＣＬ）を容易に生成し、その生成した利用権限を示すデータに基づいて電子データに対するアクセス制御を行うアクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】

かかる目的を達成するため、請求項１記載の発明は、所定のネットワークに接続されたアクセス制御サーバであって、ネットワークを介して電子データの作成者の端末から電子データを受信する電子データ受信手段と、受信された電子データのデータ種別を示す情報および受信された電子データに係るユーザのユーザＩＤを含むワークフロー情報を受信するワークフロー情報受信手段と、電子データに対するユーザの種別ごとのアクセス権限を示すアクセス権限テンプレートを電子データのデータ種別ごとに１つ以上格納するテンプレート格納手段と、格納された１つ以上のアクセス権限テンプレートから、受信されたワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出手段と、抽出されたアクセス権限テンプレートに、各ユーザのユーザＩＤを挿入して、受信された電子データに対する各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成手段と、を有することを特徴とする。

【０００８】

また、請求項２記載の発明によれば、請求項１記載のアクセス制御サーバにおいて、受信された電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信手段と、アクセス制限情報に基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成手段と、生成されたアクセス制限データをネットワークを介して送信するデータ送信手段と、を有することを特徴とする。

【０００９】

また、請求項３記載の発明によれば、請求項２記載のアクセス制御サーバにおいて、テンプレート格納手段は、ユーザの種別として、電子データの作成者、電

子データの承認者、およびアクセス制限データの送信先のユーザが設定されているアクセス権限テンプレートを格納することを特徴とする。

【００１０】

また、請求項４記載の発明によれば、請求項２または３記載のアクセス制御サーバにおいて、アクセス制限データ生成手段は、予め自サーバに格納されたセキュリティポリシーに基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする。

【００１１】

また、請求項５記載の発明によれば、請求項２から４のいずれか１項に記載のアクセス制御サーバにおいて、アクセス制限データ生成手段は、受信された電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする。

【００１２】

また、請求項６記載の発明は、所定のネットワークに接続され、電子データに対するアクセス制御を行うアクセス制御サーバを用いた電子データ発行ワークフロー処理方法であって、アクセス制御サーバが、ネットワークを介して電子データの作成者の端末から電子データを受信する電子データ受信工程と、アクセス制御サーバが、受信した電子データのデータ種別を示す情報および受信された電子データに係るユーザのユーザＩＤを含むワークフロー情報を受信するワークフロー情報受信工程と、アクセス制御サーバが、電子データに対するユーザの種別ごとのアクセス権限を示すアクセス権限テンプレートを電子データのデータ種別ごとに１つ以上格納するテンプレート格納工程と、アクセス制御サーバが、格納した１つ以上のアクセス権限テンプレートから、受信したワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出工程と、アクセス制御サーバが、抽出したアクセス権限テンプレートに、各ユーザのユーザＩＤを挿入して、受信した電子データに対する各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成工程と、を有することを特徴とする。

【００１３】

また、請求項７記載の発明によれば、請求項６記載の電子データ発行ワークフロー処理方法において、アクセス制御サーバが、受信した電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信工程と、承認情報受信後に、アクセス制御サーバが、アクセス制限情報に基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成工程と、アクセス制御サーバが、生成されたアクセス制限データをネットワークを介して送信するデータ送信工程と、を有することを特徴とする。

【００１４】

また、請求項８記載の発明によれば、請求項６記載の電子データ発行ワークフロー処理方法において、アクセス制御サーバが、アクセス制限情報に基づいて、受信した電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成工程と、アクセス制御サーバが、受信した電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信工程と、アクセス制御サーバが、承認情報を受信すると、生成されたアクセス制限データをネットワークを介して送信するデータ送信工程とを有することを特徴とする。

【００１５】

また、請求項９記載の発明によれば、請求項７または８記載の電子データ発行ワークフロー処理方法において、テンプレート格納処理は、ユーザの種別として、電子データの作成者、電子データの承認者、およびアクセス制限データの送信先のユーザが設定されているアクセス権限テンプレートを格納することを特徴とする。

【００１６】

また、請求項１０記載の発明によれば、請求項７から９のいずれか１項に記載の電子データ発行ワークフロー処理方法において、アクセス制限データ生成工程は、アクセス制御サーバが、予め自サーバに格納したセキュリティポリシーに基づいて、受信した電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする。

【００１７】

また、請求項１１記載の発明によれば、請求項７から１０のいずれか１項に記

載の電子データ発行ワークフロー処理方法において、アクセス制限データ生成工程は、受信した電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする。

【００１８】

また、請求項１２記載の発明は、電子データの作成者により作成された電子データの受信制御を行う電子データ受信処理と、受信された電子データのデータ種別を示す情報および受信された電子データに係るユーザのユーザＩＤを含むワークフロー情報の受信制御を行うワークフロー情報受信処理と、電子データに対するユーザの種別ごとのアクセス権限を示す１つ以上のアクセス権限テンプレートを電子データのデータ種別ごとに格納するテンプレート格納処理と、格納された１つ以上のアクセス権限テンプレートから、受信されたワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出処理と、抽出されたアクセス権限テンプレートに、各ユーザのユーザＩＤを挿入して、受信された電子データに対する各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成処理と、をコンピュータに実行させることを特徴とする。

【００１９】

また、請求項１３記載の発明によれば、請求項１２記載のプログラムにおいて、受信された電子データの発行が承認者により承認された旨の承認情報の受信制御を行う承認情報受信処理と、承認情報受信後に、アクセス制限情報に基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成処理と、生成されたアクセス制限データの送信制御を行うデータ送信処理と、をコンピュータに実行させることを特徴とする。

【００２０】

また、請求項１４記載の発明によれば、請求項１２記載のプログラムにおいて、アクセス制限情報に基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成処理と、受信された電子データの発行が承認者により承認された旨の承認情報の受信制御を行う承認情報受信処理と、承認情報の受信を認識すると、生成されたアクセス制限データの

送信制御を行うデータ送信処理と、をコンピュータに実行させることを特徴とする。

【００２１】

また、請求項１５記載の発明によれば、請求項１３または１４記載のプログラムにおいて、テンプレート格納処理は、ユーザの種別として、電子データの作成者、電子データの承認者、およびアクセス制限データの送信先のユーザが設定されているアクセス権限テンプレートを格納することを特徴とする。

【００２２】

また、請求項１６記載の発明によれば、請求項１３から１５のいずれか１項に記載のプログラムにおいて、アクセス制限データ生成処理は、セキュリティポリシーに基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする。

【００２３】

また、請求項１７記載の発明によれば、請求項１３から１６のいずれか１項に記載のプログラムにおいて、アクセス制限データ生成処理は、受信された電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする。

【００２４】

また、請求項１８記載の発明によれば、請求項１２から１７のいずれか１項に記載のプログラムを実行することを特徴とする。

【００２５】

また、請求項１９記載の発明によれば、請求項１２から１７のいずれか１項に記載のプログラムを記録したことを特徴とする。

【００２６】

【発明の実施の形態】

（第１の実施形態）

本実施形態において、文書発行ワークフローシステムは、発行したドキュメントを審査・承認した後、保護ドキュメントを発行する。なお、本明細書において、「ドキュメント」とは、単なる文書を示すものに限定されず、電子データによ

るものであれば、プログラム、画像、データベースまたは他のものであってもよい。

【００２７】

図１は、本発明の第１の実施形態における文書発行ワークフローシステムを示す第１の図である。以下、図１を用いて、本実施形態における文書発行ワークフローシステムの構成について説明する。

【００２８】

文書発行ワークフローシステムは、作成者端末１と、アクセス制御サーバ２と、承認者端末３と、ユーザ端末４と、を有する。また、アクセス制御サーバ２は、作成者端末１、承認者端末３、およびユーザ端末４とそれぞれネットワークを介して接続されている。

【００２９】

作成者端末１は、ドキュメント作成者により操作される情報処理装置であり、例えばパーソナルコンピュータであってもよい。作成者端末１は、表示装置（例えば、ＬＣＤ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ））と、入力装置（例えば、キーボード）と、記録装置（例えば、ＦＤＤ（Ｆｌｏｐｐｙ（登録商標）　Ｄｉｓｋ　Ｄｒｉｖｅ）、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ））とを有する。

【００３０】

また、作成者端末１は、自身に格納された作成クライアントプログラム１０を実装する。例えば、作成クライアントプログラム１０は、Ｗｅｂブラウザで実現するようにしてもよいし、他にもＩＢＭ社のグループウェア製品であるＬｏｔｕｓ　Ｎｏｔｅｓ（登録商標）のクライアント用プログラムであってもよい。

【００３１】

作成者端末１は、電子データであるドキュメント１１と、ドキュメント１１の属性等を示すワークフロー情報１２とを生成し、アクセス制御サーバ２に送信する。

【００３２】

アクセス制御サーバ２は、ドキュメント１１およびＡＣＬなどを管理する情報

処理装置であって、例えばＷｅｂサーバであってもよい。アクセス制御サーバ２は、ワークフロープログラム２０およびドキュメント保護プログラム２１により動作する。

【００３３】

また、アクセス制御サーバ２は、例えばＨＤＤなどの記録装置２２を有する。記録装置２２は、ＡＣＬテンプレートＤＢ（ＡＣＬテンプレートデータベース）２３と、ＡＣＬＤＢ（ＡＣＬデータベース）２４と、ワークフローオブジェクト２５とを格納する。

【００３４】

ＡＣＬテンプレートＤＢ２３は、ドキュメント１１の種類（ファイルタイプ）に応じた１つ以上のＡＣＬテンプレートを管理するデータベースである。ＡＣＬテンプレートとは、ドキュメント１１へのアクセス権限が示されているＡＣＬ生成時に用いられるＡＣＬのテンプレート情報である。

【００３５】

ＡＣＬＤＢ２４は、ワークフロープログラム２０が生成したＡＣＬを管理するデータベースである。

【００３６】

ワークフローオブジェクト２５は、ドキュメント１１とワークフロー情報１２ａとをそれぞれ対応付けて組み合わせた情報である。

【００３７】

承認者端末３は、ドキュメント配布の承認（ａｐｐｒｏｖｅ）または却下（ｒｅｊｅｃｔ）を判断する承認者により操作される情報処理装置であって、例えばパーソナルコンピュータであってもよい。承認者端末３は、表示装置（例えば、ＬＣＤ）と、入力装置（例えば、キーボード）と、記録装置（例えば、ＦＤＤ、ＨＤＤ）とを有する。

【００３８】

また、承認者端末３は、承認者クライアントプログラム３０を格納し、承認者クライアントプログラム３０は、承認者端末３に各動作を実行させる。

【００３９】

ユーザ端末４は、ドキュメント１１（保護ドキュメント１３）を利用するユーザにより操作される情報処理装置であって、例えばパーソナルコンピュータであってもよい。また、ユーザ端末４は、表示装置（例えば、ＬＣＤ）と、入力装置（例えば、キーボード）と、記録装置（例えば、ＦＤＤ、ＨＤＤ）とを有する。

【００４０】

以下、図１を用いて、本実施形態における文書発行ワークフローシステムによる動作について説明する。

【００４１】

まず、作成者端末１は、ドキュメント作成者が承認依頼を希望するドキュメント１１と、ドキュメント１１に係る情報が示されるワークフロー情報１２とを取得する。なお、ドキュメント１１およびワークフロー情報１２は、必ずしも作成者端末１が生成したものでなくてもよく、作成者端末１が、接続されている所定のネットワークを介して受信したものであってもよい。また、ドキュメント１１およびワークフロー情報１２が所定の携帯可能な記録媒体に記録されており、作成者端末１が、その記録媒体を読み取って取得してもよい。

【００４２】

図２は、本発明の第１の実施形態における作成者端末１のワークフロー情報１２作成時の画面表示を示す図である。作成者クライアントプログラム１０は、図２に示されるような画面を作成者端末１に設けられた表示装置の画面上に表示させる。

【００４３】

図２に示されているように、ワークフロー情報１２の生成画面には、ドキュメント１１の「ファイルタイトル」、「ファイルタイプ」、「作成者」、「ファイル内容」、「配布先」、および「承認者」の入力欄が設けられており、ドキュメント作成者は、作成者端末１に設けられている入力装置を介して、上記の各入力欄に情報を入力する。作成者クライアントプログラム１０は、各入力欄に入力された情報に基づいて、ワークフロー情報１２を生成する。

【００４４】

「ファイルタイトル」は、ドキュメント１１のタイトル（表題）を示す。また

、「ファイルタイプ」は、作成者端末１内に予め１つ以上定義および設定されており、作成者端末１は、例えばプルダウンメニューにより１種類以上のファイルタイプから所定のものを選択するようにしてもよい。「ファイル内容」には、承認を依頼するドキュメント１１のファイル名が記載されており、その記載されたファイル名のドキュメント１１がワークフロー情報１２に添付される。

【００４５】

「作成者」、「配布先」、および「承認者」の入力欄には、該当するユーザのユーザＩＤを入力する。例えば、図２に示されているように、ユーザＩＤとして、各ユーザのメールアドレスを入力するようにしてもよい。なお、ユーザの種別は「作成者」、「配布先」、および「承認者」に限定されず、また各ユーザの数についても図２に示されるものに限定されない。

【００４６】

図３は、本発明の第１の実施形態におけるワークフロー情報１２の一例を示す図である。図２に示されるような入力情報に基づいて、図３に示されるようなワークフロー情報１２が生成される。図３に示されているように、ワークフロー情報１２には、ドキュメント１１のファイルタイトル「Ｄｅｖｅｌｏｐｍｅｎｔ ｏｆ ａ ｎｅｗ ｓｅｃｕｒｉｔｙ ｓｙｓｔｅｍ」と、ファイルタイプ「ＲＥＳＥＡＲＣＨ＿ＰＬＡＮ」と、作成者「ａｕｔｈｏｒ＿００@ｏｆｆｉｃｅ．ｃｏｍ」と、承認者「ａｐｐｒｏｖｅｒ＿０１@ｏｆｆｉｃｅ．ｃｏｍ」と、ファイル内容（ドキュメントのファイル名）「ｔｈｅｍｅ＿ｅｘｐｌａｎａｔｉｏｎ．ｄｏｃ」と、配布先「ｕｓｅｒ＿１０@ｏｆｆｉｃｅ．ｃｏｍ，ｕｓｅｒ＿１１@ｏｆｆｉｃｅ．ｃｏｍ，ｕｓｅｒ＿２０@ｏｆｆｉｃｅ．ｃｏｍ，ｕｓｅｒ＿２１@ｏｆｆｉｃｅ．ｃｏｍ」といった情報が含まれている。

【００４７】

なお、ワークフロー情報１２の内容は、図３に示されるものに限定されず、他の内容の情報であってもよい。また、図３で、「ファイル内容」のところには承認を依頼するドキュメント１１のファイル名が記載されているが、実際には、ドキュメント１１のファイルそのものを示す。

【００４８】

次に、作成者端末１は、ドキュメント１１およびワークフロー情報１２をアクセス制御サーバ２に送信し、ワークフローに流す。具体的には、作成者クライアントプログラム１０は、図２のワークフロー情報１２作成画面上に設けられている「承認（審査）依頼」ボタンのクリックを検出すると、ワークフロー情報１２を生成し、生成したワークフロー情報１２とともに対応するドキュメント１１をアクセス制御サーバ２に送信するとしてもよい。

【００４９】

アクセス制御サーバ２は、作成者端末１からドキュメント１１およびワークフロー情報１２を受信すると、ワークフロープログラム２０は、受信したワークフロー情報１２に対してユニーク（固有）なドキュメントＩＤ（シリアル番号でも良い）を付与し、図４に示されるような例えばＸＭＬで記述したファイル（ワークフロー情報１２ａ）を作成して、アクセス制御サーバ２内の記録装置（ＨＤＤ）２２にドキュメント１１とともに保存する。このとき、ドキュメント１１とそれに対応するワークフロー情報１２ａとを関連付けた一組のデータをワークフローオブジェクト２５とする。

【００５０】

図４は、本発明の第１の実施形態におけるＩＤが付与されたワークフロー情報１２ａを示す図である。図４に示されているように、ワークフロー情報１２ａには、固有なドキュメントＩＤ「０１１２３７８３５」が付与されている。また、ワークフロー情報１２ａの現在の状態を示す「＜ｓｔａｔｕｓ＞」には、「ｗａｉｔ＿ｆｏｒ＿ａｐｐｒｏｖａｌ（承認待ち）」が示されており、図４に示されるワークフロー情報１２ａに対応するドキュメント１１が承認者による審査（承認／却下）の結果を待っている状態であることが示されている。

【００５１】

次に、ワークフロープログラム２０は、ワークフロー情報１２ａに記載されている承認者端末３（承認者のメールアドレス）に承認依頼の電子メールを送信する。承認依頼の電子メールには、ワークフロー情報１２ａに付与されたユニークなドキュメントＩＤを記載する。また、アクセス制御サーバ２をＷｅｂサーバとし、ワークフロープログラム２０をＷｅｂサーバで稼動するプログラムとして実

現する場合、ワークフロープログラム２０は、ワークフローオブジェクト２５に該当するＵＲＬ（例えばｈｔｔｐ：／／ｓｅｒｖｅｒ／ｗｏｒｋｆｌｏｗ？ｗｆｉｄ＝０１１２３７８３５）を電子メールに記載して承認者端末３に送信するようにしてもよい。

【００５２】

図５は、本発明の第１の実施形態における文書発行ワークフローシステムを示す第２の図である。以下、図５を用いて、本実施形態における文書発行ワークフローシステムによる動作の説明を続ける。

【００５３】

承認者端末３は、アクセス制御サーバ２から承認を依頼されているワークフローオブジェクト２５が示されている電子メールを受信すると、承認者クライアントプログラム３０を用いて、アクセス制御サーバ２に格納されているワークフローオブジェクト２５の一覧を承認者端末３に設けられている表示装置の画面上に表示し、上記の電子メールにより承認を求められているワークフローオブジェクト２５を選択する。

【００５４】

承認者端末３は、承認者により例えば承認者端末３の入力装置に設けられている「承認ボタン」または「却下ボタン」が押下されたことを検出すると、必要に応じてワークフロー情報１２ａを改訂した上でワークフローオブジェクト２５の「承認（Ａｐｐｒｏｖｅ）」または「却下（Ｒｅｊｅｃｔ）」を決定した旨の情報を認識する。

【００５５】

承認者クライアントプログラム３０は、ワークフローオブジェクト２５に対して「承認」および「却下」のうちのどちらに決定されたかを判断し、「却下」されたことを認識すると（例えば却下ボタンが押されると）、却下されたこと（Ｒｅｊｅｃｔｅｄ）を示す情報をアクセス制御サーバ２に送信する。アクセス制御サーバ２は、却下されたことを示す情報を受信すると、ワークフローオブジェクト２５が却下されたことを示す情報を電子メールなどで作成者端末１に送信し、文書発行ワークフローシステムは、動作を終了する。

【００５６】

承認者クライアントプログラム３０は、ワークフローオブジェクト２５が「承認」されたことを認識すると（例えば承認ボタンが押されると）、承認されたこと（Ａｐｐｒｏｖａｌ）を示す情報をアクセス制御サーバ２に送信する。

【００５７】

ワークフロープログラム２０は、アクセス制御サーバ２が承認された旨の情報を受信したことを認識すると、Ａｐｐｒｏｖａｌの対象となっているワークフローオブジェクト２５についてワークフロー情報１２ａを改訂して、ワークフローの状態を示す項目（＜ｓｔａｔｕｓ＞）を「承認済み（Ａｐｐｒｏｖｅｄ）」にする。

【００５８】

次に、ワークフロープログラム２０は、ワークフロー情報１２ａを「承認済み」にすると、その「承認済み」にしたワークフロー情報１２ａに基づいて、配布文書（ドキュメント１１）のＡＣＬを生成する。そのＡＣＬの生成は例えば以下のようにして行う。なお、ワークフロー情報１２ａの内容は、図４に示されているものとする。

【００５９】

図４に示されているワークフロー情報１２ａにおいて、承認されたドキュメント１１のファイルタイプは、「ＲＥＳＥＡＲＣＨ＿ＰＬＡＮ」であり、承認された後、＜ｄｉｓｔｒｉｂｕｔｅ＿ｔｏ＞で列挙されている相手（配布先）のユーザ端末４に配布されることを表している。この例ではユーザＩＤとして電子メールアドレスを用いている。

【００６０】

本実施形態では、アクセス制御サーバ２は、予め「ＲＥＳＥＡＲＣＨ＿ＰＬＡＮ」、「ＣＯＮＴＲＡＣＴ」、「ＴＯＰ＿ＳＥＣＲＥＴ」などのファイルタイプごとにＡＣＬのテンプレートを格納しておく。なお、ここで挙げたファイルタイプはあくまでも一例であり、その名称および数などは他のものであってもよい。

【００６１】

図６は、本発明の第１の実施形態におけるＡＣＬテンプレートを示す図である

。図６には、ファイルタイプが「ＲＥＳＥＡＲＣＨ＿ＰＬＡＮ」であるドキュメントに対するＡＣＬテンプレートが示されている。

【００６２】

図６に示されているように、ＡＣＬテンプレートには例えば「Ｕｓｅｒ　ｔｙｐｅ（ユーザタイプ）」、「Ａｃｃｅｓｓ　ｔｙｐｅ（アクセスタイプ）」、「Ｐｅｒｍｉｓｓｉｏｎ（許可情報）」、および「Ｒｅｑｕｉｒｅｍｅｎｔｓ（処理要件）」といった項目がある。

【００６３】

「ユーザタイプ」は、ドキュメントに対するアクセス権限を有するユーザの種類を示す項目であり、本実施形態では、「ａｕｔｈｏｒ（ドキュメント作成者）」、「Ａｐｐｒｏｖｅｒ（承認者）」、「ｄｉｓｔｒｉｂｕｔｅ＿ｔｏ（配布先のユーザ）」に区分されている。

【００６４】

「アクセスタイプ」は、ドキュメントに対するアクセス方法の種類を示す項目であり、本実施形態では、「Ｒｅａｄ（ドキュメントの閲覧）」、「Ｗｒｉｔｅ（ドキュメントの書き換え）」、「Ｐｒｉｎｔ（ドキュメントの印刷）」、「Ｈａｒｄｃｏｐｙ（ドキュメントのハードコピー）」に区分されている。

【００６５】

「許可情報」は、ドキュメント１１のアクセスに対するＡｌｌｏｅｗｄ（許可）／Ｄｅｎｉｅｄ（禁止）をユーザの種類（Ｕｓｅｒ　ｔｙｐｅ）ごとに示すものである。例えば、図６に示されるＡＣＬテンプレートでは、「ａｕｔｈｏｒ（ドキュメント作成者）」は、「Ｒｅａｄ」、「Ｐｒｉｎｔ」、および「Ｈａｒｄｃｏｐｙ」に関してアクセスが許可されており、「Ｗｒｉｔｅ」に関してアクセスが禁止されている。

【００６６】

「処理要件」は、ユーザ端末４が保護ドキュメント１３を使用する際に、各アクセスタイプで要求される処理が示されている。例えば、図６のＡＣＬテンプレートでは、「処理要件」として、「ＰＡＣ（Ｐｒｉｖａｔｅ　Ａｃｃｅｓｓ）」、「ＢＤＰ（Ｂａｃｋｇｒｏｕｎｄ　Ｄｏｔ　Ｐａｔｔｅｒｎ）」、「ＥＢＣ（

Ｅｍｂｅｄｄｉｎｇ　Ｂａｒｃｏｒｄ）」、および「ＲＡＤ（Ｒｅｃｏｒｄ　Ａｕｄｉｔ　Ｄａｔａ）」が示されている。なお、「ＰＡＣ」、「ＢＤＰ」、「ＥＢＣ」、および「ＲＡＤ」については、後ほど詳述する。

【００６７】

ワークフロープログラム２０は、ワークフロー情報１２ａの「＜ｓｔａｔｕｓ＞」を「Ａｐｐｒｏｖａｌ（承認済み）」にした後、記録装置２２内のＡＣＬテンプレートＤＢ２３で管理されている１つ以上のＡＣＬテンプレートから、ワークフロー情報１２ａに記述されているファイルタイプに対応したＡＣＬテンプレートを抽出する。本実施形態では、図５のように「ファイルタイプ」が「ＲＥＳＥＡＲＣＨ＿ＰＬＡＮ」であるワークフロー情報１２ａに基づいて、ワークフロープログラム２０は、図６に示されるような「ＲＥＳＥＡＲＣＨ＿ＰＬＡＮ」のＡＣＬテンプレートを抽出する。

【００６８】

次に、ワークフロープログラム２０は、抽出したＡＣＬテンプレートに、ワークフロー情報１２ａに記述されている「作成者」、「承認者」、および「配布先」の情報（ユーザＩＤ）を挿入して、図７に示されるようなＡＣＬを生成する。

【００６９】

図７は、本発明の第１の実施形態におけるＡＣＬの一例を示す図である。図７には、ワークフロー情報１２ａに示される「作成者」、「承認者」、および「配布先」（「ａｕｔｈｏｒ＿００@ｏｆｆｉｃｅ．ｃｏｍ」、「ａｐｐｒｏｖｅｒ＿０１@ｏｆｆｉｃｅ．ｃｏｍ」、「ｕｓｅｒ＿１０@ｏｆｆｉｃｅ．ｃｏｍ」、「ｕｓｅｒ＿１１@ｏｆｆｉｃｅ．ｃｏｍ」、「ｕｓｅｒ＿２０@ｏｆｆｉｃｅ．ｃｏｍ」、「ｕｓｅｒ＿２１@ｏｆｆｉｃｅ．ｃｏｍ」）それぞれにおけるアクセス権限が示されている。

【００７０】

ワークフロープログラム２０は、生成したＡＣＬを、生成時に用いたワークフロー情報１２ａに記述されていたドキュメントＩＤに関連付けてＡＣＬＤＢ２４に登録する。

【００７１】

ワークフロープログラム２０は、このようにして生成したＡＣＬと、ドキュメント１１とをドキュメント保護プログラム２１に渡す。ドキュメント保護プログラム２１は、生成されたＡＣＬに基づいて、ドキュメント１１をプロテクトし、保護ドキュメント１３を生成する。

【００７２】

ワークフロープログラム２０は、生成された保護ドキュメント１３を取得し、取得した保護ドキュメント１３を、配布先に指定されたユーザのユーザ端末４に電子メールなどで配布する。このとき、アクセス制御サーバ２は、保護ドキュメント１３そのものをユーザ端末４に配布してもよい。

【００７３】

ここで、図５を用いて、本実施形態におけるＡＣＬを用いたドキュメント１１に対するセキュリティ処理について説明する。なお、ユーザ端末４には、ドキュメントアクセスプログラムが実装されている。また、ユーザ端末４にはプリンタが接続されていることとする。

【００７４】

ドキュメント保護プログラム２１は、ドキュメント１１にアクセス制御サーバ２の使用者（配布者）の入力操作に応じた処理要件を設定するとともに、暗号化アルゴリズム（ＲＣ４、Ｔｒｉｐｌｅ　ＤＥＳ、ＩＤＥＡなど）を用いてドキュメント１１を暗号化し、保護ドキュメント１３を生成する処理を行う。

【００７５】

ドキュメントアクセスプログラムは、ユーザ端末４の使用者（ユーザ）の入力操作に応じ、保護ドキュメント１３を復号化するとともに設定されている処理要件に応じた印刷処理を自身で行うか、あるいはプリンタなどに実行させる処理を行うプログラムである。

【００７６】

アクセス制御サーバ２は、ユーザがドキュメントを印刷しようとする場合に、ドキュメントアクセスプログラムからの要求に応じてＡＣＬを参照し、ドキュメントにアクセスする権限があるか否か、処理要件がどのように設定されているかを取得するサーバである。

また、アクセス制御サーバ２は、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベースをさらに有するとする。

【００７７】

ドキュメント保護プログラム２１は、ドキュメント１１およびＡＣＬを取得すると、復号に使用する暗号鍵（Ｋｅｙ）を生成し、生成した暗号鍵を該当するドキュメントＩＤに関連づけて、記録装置２２に登録する。

また、ドキュメント保護プログラム２１は、暗号鍵を用いてドキュメント１１を暗号化し、暗号化したドキュメント１１に対してドキュメントＩＤを付加して保護ドキュメント１３を生成する。

【００７８】

アクセス制御サーバ２は、生成した保護ドキュメント１３をネットワークを介して送信するなどしてユーザ端末４に渡す。

【００７９】

ユーザが、ユーザ端末４の入力装置を介してドキュメントアクセスプログラムに対してドキュメントへのアクセスを指示すると、アクセスを要求されたドキュメントアクセスプログラムは、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメントアクセスプログラムは、ユーザ端末４の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。

【００８０】

ドキュメントアクセスプログラムは、ユーザから入力されたユーザ名とパスワードとをアクセス制御サーバ２へ送信して、ユーザ認証を要求する。

【００８１】

アクセス制御サーバ２は、ドキュメントアクセスプログラムから受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

ユーザを特定すると、アクセス制御サーバ２は、ＡＣＬＤＢ２４を参照し、ドキュメント１１にアクセスする権限が配布先のユーザにあるか否かや、ユーザがドキュメント１１にアクセスする際には、どのような処理要件が設定されているかを取得する。

ユーザにドキュメント１１にアクセスする権限がある場合、アクセス制御サーバ２は、その旨を示す認証情報とともに、保護ドキュメント１３を復号化するための暗号鍵とユーザがドキュメント１１にアクセスする際の処理要件とをユーザ端末４を介してドキュメントアクセスプログラムに通知する。

【００８２】

アクセス制御サーバ２から認証情報とともに、暗証鍵と処理要件とを取得したドキュメントアクセスプログラムは、暗号鍵を用いて保護ドキュメント１３を復号化してドキュメント１１に復元する。

ここで、ユーザがドキュメント１１の印刷を要求している場合、ドキュメントアクセスプログラムは、処理要件を満たすようにプリンタに印刷処理を実行させる。例えば、保護ドキュメント１３にＢＤＰが処理要件として設定されている場合には、ドキュメント１１の内容とともに地紋を印刷する。

【００８３】

これにより、ドキュメント１１を印刷する際に、配布者がユーザ各人に対して設定した処理要件を強制することが可能となる。

【００８４】

また、アクセス制御サーバ２は、保護ドキュメント１３をワークフローオブジェクト２５の一部として記録装置２２に保存しておき、その保護ドキュメント１３にアクセスするためのＵＲＬを電子メールでユーザ端末４に送るようにしてもよい（例えばｈｔｔｐ：／／ｓｅｒｖｅｒ／ｗｏｒｋｆｌｏｗ？ｗｆｉｄ＝０１１２３７８３５など）。

【００８５】

また、アクセス制御サーバ２は、ユーザ端末４と同様に、作成者端末１および承認者端末３に対しても保護ドキュメント１３またはＵＲＬを送信するとしてもよい。

【００８６】

上記のようにして、アクセス制御サーバ２は、承認されたドキュメントのアクセス権限を制限し、配布先のユーザにはアクセス制限のかかった保護ドキュメントを配布する。従って、アクセス制御サーバ２は、アクセス権限のあるユーザだ

けにドキュメントの内容の参照を許可し、また、印刷時においても権限を確認したうえでセキュリティ処理を施しながらアクセス権限を有するユーザに印刷させることができる。

【００８７】

また、ドキュメント１１が保護ドキュメント１３を作成するのにふさわしくないデータフォーマットである場合、ワークフロープログラム２０は、ドキュメント１１から最適なデータフォーマットのドキュメントへの変換処理をあらかじめ施し、変換したドキュメントをドキュメント保護プログラム２１に渡すようにするとよい。例えば、ドキュメント１１がＭｉｃｒｏｓｏｆｔ　Ｗｏｒｄ（登録商標）のファイルであって、ドキュメント保護プログラム２１にとって最適なデータフォーマットがＰＤＦファイルである場合、ワークフロープログラム２０は、Ｍｉｃｒｏｓｏｆｔ　Ｗｏｒｄを起動して、ＷｏｒｄファイルをＡｄｏｂｅ　Ａｃｒｏｂａｔ（登録商標）の機能を使ってＰＤＦに変換した上で、ドキュメント保護プログラム２１に渡す。従って、作成者端末１が作成するドキュメント１１のデータフォーマットは、ＰＤＦに変換することができるものであれば何でも良いということになる。

【００８８】

また、上記の実施形態では、アクセス制御サーバ２は、承認された後でドキュメント１１から保護ドキュメント１３を生成しているが、アクセス制御サーバ２がワークフロー情報１２ａを承認者端末３に「＜ｓｔａｔｕｓ＞」以外の部分を変更させない、つまり変更が必要な場合にはドキュメント１１を却下するとしてもよい。その場合、アクセス制御サーバ２は、承認者端末３により審査（承認／却下）される前にあらかじめ保護ドキュメント１３を生成しておき、生成した保護ドキュメント１３をワークフローオブジェクト２５の一部として保存しておくようにしてもよい。

【００８９】

ここで、本実施形態における各印刷処理（「ＰＡＣ」、「ＢＤＰ」、「ＥＢＣ」、および「ＲＡＤ」）について説明する。

【００９０】

図８は、本発明の第１の実施形態におけるユーザ端末４０２による印刷動作を示す図である。図８に示されているように、ユーザ端末４０２は、ドキュメント印刷プログラム４２１と、プリンタドライバとを有する。また、ユーザ端末４０２は、プリンタ４０３と接続されている。

【００９１】

また、図９は、本発明の第１の実施形態におけるユーザ端末４０２に設けられている表示装置の画面上に表示されるプリントダイアログを示す図である。以下、図８および図９を用いて、印刷要件としてＰＡＣが設定されている場合のドキュメント印刷プログラム４２１の動作について説明する。

【００９２】

（１）ドキュメント印刷プログラム４２１はＰＡＣが設定されているドキュメントを印刷する際には、図９に示すように、プリントダイアログを表示させた後に個人識別番号（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ：ＰＩＮ）を入力するダイアログをユーザ端末４０２の表示装置に表示させ、ユーザにＰＩＮの入力を要求する。

（２）ユーザ端末４０２の入力装置を用いてユーザがＰＩＮを入力すると、ドキュメント印刷プログラム４２１は、これをプリンタドライバに設定し、印刷を指示する。

プリンタドライバは、ドキュメントからＰｏｓｔｓｃｒｉｐｔなどのＰＤＬ（Ｐａｇｅ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｌａｎｇｕａｇｅ）で記述された印刷データ（ＰＤＬデータ）を生成し、印刷部数や出力トレイなどの印刷ジョブ情報を記述したＰＪＬ（Ｐｒｉｎｔ　Ｊｏｂ　Ｌａｎｇｕａｇｅ）データをＰＤＬデータの先頭に付加する。プリンタドライバはさらにＰＪＬデータの一部としてＰＩＮを付加し、そのＰＪＬデータ付きＰＤＬデータをプリンタ４０３に送る。

プリンタ４０３は、ＰＪＬデータ付きＰＤＬデータを受け取るとＰＪＬデータの内容を参照し、機密印刷用のＰＩＮが含まれている場合は印刷出力せずにプリンタ４０３内部の記憶装置（ＨＤＤなど）にＰＪＬデータ付きＰＤＬデータを保存する。ユーザがＰＩＮをプリンタ４０３のオペレーションパネルを介して入力すると、プリンタ４０３は入力されたＰＩＮをＰＪＬデータに含まれるＰＩＮと

照合し、一致すればＰＪＬデータに含まれていた印刷ジョブ条件（部数、トレイなど）を適用しながらＰＤＬデータに従って印刷出力する。

（３）プリンタドライバにＰＩＮが設定できない、すなわち、プリンタ４０３が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。

【００９３】

このようにすることで、印刷実行後、プリンタ４０３のオペレーションパネルにおいて印刷実行前に入力したものと同一のＰＩＮが入力されるまでドキュメントのプリントアウトがプリンタ４０３から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ４０３に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。

さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ４０３とやりとりをＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）で保護してもよい。

【００９４】

また、ドキュメント印刷プログラム４２１をＷｉｎｄｏｗｓ（登録商標）　Ｄｏｍａｉｎのユーザ管理と連動させて、ユーザに対してＰＩＮの入力を要求しないようにしてもよい。例えば、ＰＩＮをユーザに入力させるのではなく、Ｗｉｎｄｏｗｓ（登録商標）　Ｄｏｍａｉｎから現在ログオン中のユーザＩＤを取得し、プリントデータとともにユーザＩＤをプリンタ４０３へ送付するようにする。プリンタ４０３は、オペレーションパネルでユーザからのパスワード入力を受け、そのユーザＩＤとパスワードとでＷｉｎｄｏｗｓ（登録商標）　Ｄｏｍａｉｎのユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。Ｗｉｎｄｏｗｓ（登録商標）　Ｄｏｍａｉｎに限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒なＰＩＮ入力の手間を削減できる。

【００９５】

次に、印刷要件としてＥＢＣが設定されている場合のドキュメント印刷プログ

ラム４２１の動作について説明する。

（１）ドキュメント印刷プログラム４２１は、ＥＢＣが設定されているドキュメントを印刷する際にドキュメントＩＤを示すバーコード画像データ（又は、二次元コード）のデータを生成する。

（２）ドキュメント印刷プログラム４２１は、生成したバーコード画像データをスタンプ画像としてプリンタドライバにセットし、プリンタ４０３に印刷を指示する。

（３）プリンタドライバにＥＢＣが設定できない、すなわち、プリンタ４０３がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【００９６】

このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキャナのみがバーコードをデコードすることでドキュメントＩＤを取得し、そのドキュメントＩＤを基にハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキュリティ確保が可能となる。

【００９７】

次に、印刷要件としてＢＤＰが設定されている場合のドキュメント印刷プログラム４２１の動作について説明する。

（１）ドキュメント印刷プログラム４２１は、ＢＤＰが設定されているドキュメントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する（例えば、Ｉｃｈｉｒｏ，２００２／０８／０４　２３：４７：１０）。

（２）ドキュメント印刷プログラム４２１は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。

（３）ドキュメント印刷プログラム４２１は、生成した地紋画像をスタンプと

してプリンタドライバにセットし、プリンタ４０３にドキュメントの印刷を指示する。

（４）プリンタドライバにＢＤＰが設定できない場合、すなわちプリンタ４０３が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【００９８】

このようにすることで、ドキュメントのプリントアウトの各ページには、印刷処理を実行したユーザ名と日時とが浮き出る地紋として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これは、ＥＢＣをサポートしていない複写機を使用する場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。

【００９９】

また、「ＲＡＤ」は、アクセス制御サーバ２内の保護ドキュメント１３にアクセスしたユーザのログを記録する処理である。

【０１００】

以上説明したように、本実施形態によれば、ドキュメント１１に係るユーザＩＤ、およびファイルタイプなどが示されているワークフロー情報１２ａと、ＡＣＬテンプレートと、を用いてＡＣＬを生成する。従って、ドキュメント１１に係るユーザＩＤおよびファイルタイプなどの簡単な情報を入力するだけで、ドキュメント１１に対する複数のユーザのＡＣＬを容易に生成することが可能となる。

【０１０１】

（第２の実施形態）

本発明の第１の実施形態では、ドキュメントのタイプ（ファイルタイプ）ごとにＡＣＬテンプレートを設定しておく例を説明した。本実施形態では、所定のセキュリティポリシーに基づいて、保護ドキュメント１３を保護する。

【０１０２】

図１０に、アクセス制御サーバ２の記録装置２２に登録されるセキュリティポリシーの一例を示す。

例えば、分野（Ｃａｔｅｇｏｒｙ）が「技術文書（Ｔｅｃｈｎｉｃａｌ）」で機密レベル（Ｓｅｎｓｉｔｉｖｉｔｙ）が「中（Ｍｅｄｉｕｍ）」のドキュメント１１は、カテゴリ（Ｃａｔｅｇｏｒｙ）が「技術（Ｔｅｃｈｎｉｃａｌ）」で階級（Ｌｅｖｅｌ）が「中（Ｍｅｄｉｕｍ）」又は「上（Ｈｉｇｈ）」のユーザに対して、閲覧（Ｒｅａｄ）は許可するがＲＡＤを要件とすること、印刷（Ｐｒｉｎｔ）を許可するがＰＡＣとＢＤＰとＥＢＣとＲＡＤとを要件とすること、及び、ハードコピー（Ｈａｒｄｃｏｐｙ）は許可しないことが規定されている。

アクセス制御サーバ２は、セキュリティポリシーのデータをどのような形で記録保持していても構わない。なお、ＸＭＬを用いて記述してもよい。

【０１０３】

図１１は、本発明の第２の実施形態におけるドキュメント１１のファイルタイプとセキュリティポリシーとの対応を示すマッピングテーブルを示す図である。図１１のようなマッピングテーブルは、アクセス制御サーバ２内の記録装置２２に格納されている。

【０１０４】

図１１に示されているように、マッピングテーブルでは、ドキュメントのファイルタイプと、Ｓｅｃｕｒｉｔｙ　ａｔｔｒｉｂｕｔｅｓ（セキュリティ属性）とが関連付けられている。セキュリティ属性には、「Ｃａｔｅｇｏｒｙ（分野）」および「Ｓｅｎｓｉｔｉｖｉｔｙ（機密レベル）」が含まれる。

【０１０５】

以下、図５を用いて、セキュリティポリシーをそのままの形で電子的に記述したものをドキュメント１１の保護に適用した場合について説明する。また、ユーザ端末４には、表示装置（例えば、ＬＣＤ）、入力装置（例えば、キーボード）、記録装置（例えば、ＦＤＤ、ＨＤＤ）などを備えたコンピュータ端末を適用できる。なお、ユーザ端末４にはドキュメント１１に対するアクセスを行うためのドキュメントアクセスプログラムが実装されている。また、ユーザ端末４には、プリンタが接続されていることとする。

【０１０６】

ドキュメントアクセスプログラムは、ユーザ端末４の使用者（ユーザ）の入力

操作に応じ、保護ドキュメント１３を復号化するとともに、設定されている処理要件に応じた処理を自身で行うか、あるいはプリンタなどに実行させる処理を行うプログラムである。

【０１０７】

ドキュメント保護プログラム２１は、アクセス制御サーバ２の管理者（ドキュメント１１の配布者）の入力操作に応じた処理要件を設定するとともに、暗号化アルゴリズム（ＲＣ４、Ｔｒｉｐｌｅ　ＤＥＳ、ＩＤＥＡなど）を用いてドキュメント１１を暗号化し、保護ドキュメント１３を生成する処理を行う。

【０１０８】

アクセス制御サーバ２は、ユーザ端末４のユーザがドキュメント１１（保護ドキュメント１３）にアクセスしようとする場合に、自身が記録保持しているセキュリティポリシーを参照し、保護ドキュメント１３にアクセスする権限があるか否か、処理要件がどのように設定されているかを取得する。アクセス制御サーバ２は、セキュリティポリシーのデータをどのような形で記録保持していても構わない。なお、セキュリティポリシーのデータは、ＸＭＬを用いて記述されていてもよい。

【０１０９】

アクセス制御サーバ２は、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベースと、各保護ドキュメント１３にどのようなセキュリティ属性が設定されているかを示す情報及びその保護ドキュメント１３を復号化する為の暗証鍵が関連づけられて登録されるセキュリティ属性データベースと、セキュリティポリシー（例えば図１０）と、ファイルタイプとセキュリティ属性の対応を示すマッピングテーブル（例えば図１１）と、を有する。

【０１１０】

ユーザデータベースは、ユーザごとにカテゴリと階級とを別々の属性として管理する。例えば、Ｗｉｎｄｏｗｓ（登録商標）　Ｄｏｍａｉｎのユーザ管理機構を利用してユーザを管理するような場合には、グループアカウントとしてＴｅｃｈｎｉｃａｌ＿Ｍｅｄｉｕｍのようなものを生成し、Ｉｃｈｉｒｏというユーザをそのグループに所属させるようにしてもよい。所属グループの命名規則をこの

ように設定しておくことで、カテゴリと階級とを管理することが可能となる。

【０１１１】

以下、セキュリティポリシーを用いて、ドキュメント１１にセキュリティ処理を施す場合の文書発行ワークフローシステムの動作を説明する。

【０１１２】

ワークフロープログラム２０は、ワークフロー情報１２ａ生成後、ファイルタイプとセキュリティ属性とが関連付けられているマッピングテーブルを参照して、ワークフロー情報１２ａで指定されたファイルタイプに対応したセキュリティ属性と、ドキュメント１１とをドキュメント保護プログラム２１に渡す。例えば、ワークフロー情報１２ａでＲＥＳＥＡＲＣＨ＿ＰＬＡＮが指定された場合には、ワークフロープログラム２０は、ドキュメント１１およびそのドキュメントＩＤとともに、図１１のテーブルに基づいたセキュリティ属性として「Ｔｅｃｈｎｉｃａｌ」と「Ｍｅｄｉｕｍ」をドキュメント保護プログラム２１に渡す。

【０１１３】

セキュリティ属性を取得したドキュメント保護プログラム２１は、復号に使用する暗号鍵を生成し、生成した暗号鍵とセキュリティ属性とをドキュメントＩＤに関連づけて記録装置２２に登録する。

また、ドキュメント保護プログラム２１は、暗号鍵を用いて暗号化したドキュメント１１に対してドキュメントＩＤを付加して保護ドキュメント１３を生成する。

【０１１４】

アクセス制御サーバ２は、ドキュメント保護プログラム２１が生成した保護ドキュメント１３を例えばネットワークを介して送信するなどしてユーザ端末４に受け渡す。

【０１１５】

ユーザが、ユーザ端末４に対して保護ドキュメント１３へのアクセスを指示すると、アクセス要求されたユーザ端末４は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメントアクセスプログラムは、ユーザ端末４の表示装置にメッセージを表示するなどして、ユ

ーザ名とパスワードの入力を要求する。

【０１１６】

ドキュメントアクセスプログラムは、ユーザから入力されたユーザ名とパスワードとをアクセス制御サーバ２へ送信して、ユーザ認証を要求する。

【０１１７】

アクセス制御サーバ２は、ユーザ端末４から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【０１１８】

ユーザを特定すると、アクセス制御サーバ２は、セキュリティ属性データベースを参照し、保護ドキュメント１３に設定されているセキュリティ属性の種類を特定する。

アクセス制御サーバ２は、ユーザＤＢから取得したユーザの階級を示す情報及び、ドキュメント１１に設定されているセキュリティ属性とに基づいて、ドキュメント１１に対するアクセス権限がユーザにあるか否かや、ユーザがドキュメント１１にアクセスする際にはどのような処理要件が設定されているのかを取得する。

【０１１９】

ユーザにドキュメント１１にアクセスする権限がある場合、アクセス制御サーバ２は、アクセスが許可されていることを示す許可情報とともに、保護ドキュメント１３を復号化するための暗号鍵とユーザがドキュメント１１にアクセスする際の処理要件とをユーザ端末４へ送信し、ドキュメントアクセスプログラムに受け渡す。

【０１２０】

アクセス制御サーバ２から許可情報とともに、暗証鍵と処理要件とを取得したドキュメントアクセスプログラムは、暗号鍵を用いて保護ドキュメント１３を復号化してドキュメント１１に復元する。

例えば、ドキュメントアクセスプログラムは、ドキュメント１１の印刷を行う場合、処理要件を満たすように自身に接続されているプリンタに印刷処理を実行させる。例えば、ドキュメント１１にＢＤＰが印刷の処理要件として設定されて

いる場合には、ドキュメント１１の内容とともに地紋画像を印刷する。

【０１２１】

これにより、ドキュメント１１を印刷する際に、予め設定されたセキュリティ属性に応じた処理要件を強制することが可能となる。

【０１２２】

なお、本発明の第１および第２の実施形態では、ワークフロープログラム２０とドキュメント保護プログラム２１とは、アクセス制御サーバ２に格納され、アクセス制御サーバ２を動作させていたが、それぞれ異なった情報処理装置に格納され、それぞれの情報処理装置を動作させるようにしてもよい。

【０１２３】

以上説明したように、本実施形態では、アクセス制御サーバ２は、ファイルタイプとセキュリティ属性とを関連付けたテーブルを格納する。従って、ドキュメント１１に係るユーザＩＤおよびファイルタイプなどの簡単な情報を入力するだけで、セキュリティポリシーに基づいた複数のユーザに対するドキュメント１１へのアクセス制御を容易に行うことが可能となる。

【０１２４】

また、作成クライアントプログラム１０は、ドキュメント１１およびワークフロー情報１２を作成する処理と、ワークフロー情報１２作成画面をディスプレイに表示させる処理と、ドキュメント１１およびワークフロー情報１２を送信させる処理と、を作成者端末１のコンピュータに実行させる。

【０１２５】

また、ワークフロープログラム２０は、ワークフロー情報１２ａを生成する処理と、承認者端末３にドキュメント１１の審査を依頼する旨の情報を送信させる処理と、承認者端末３からの「承認」または「却下」を示す情報に基づいてワークフロー情報１２ａを書き換える処理と、ＡＣＬテンプレートを格納する処理と、承認されたドキュメントの種別のＡＣＬテンプレートを抽出する処理と、抽出したＡＣＬテンプレートに各ユーザ（作成者、承認者、および配布先）に係る情報を挿入してドキュメント１１のアクセス権限を示すＡＣＬを生成する処理と、暗号鍵を生成する処理と、ドキュメント１１のセキュリティ属性を抽出する処理

と、ドキュメント１１のデータフォーマットを変換する処理と、保護ドキュメント１３を送信させる処理と、をアクセス制御サーバ２に実行させる。

【０１２６】

また、ドキュメント保護プログラム２１は、ドキュメント１１および対応するＡＣＬ（またはセキュリティポリシー）に基づいて、プロテクトされたドキュメントである保護ドキュメント１３を生成する処理と、をアクセス制御サーバ２のコンピュータに実行させる。

【０１２７】

また、承認者クライアントプログラム３０は、情報の送受信を制御する処理と、情報の表示を制御する処理と、ドキュメントが「承認」または「却下」された旨の情報入力を認識する処理と、「承認」または「却下」された旨の情報の送信を制御する処理と、を承認者端末３のコンピュータに実行させる。

【０１２８】

また、ドキュメントアクセスプログラムは、情報の送受信を制御する処理と、保護ドキュメント１３を復元する処理と、プリンタに印刷を指示する処理と、をユーザ端末４に実行させる。

【０１２９】

上記の作成者クライアントプログラム１０、ワークフロープログラム２０、ドキュメント保護プログラム２１、承認者クライアントプログラム３０、およびドキュメントアクセスプログラムは、光記録媒体、磁気記録媒体、光磁気記録媒体、または半導体等の記録媒体に記録され、上記の記録媒体からロードされるようにしてもよいし、所定のネットワークを介して接続されている外部機器からロードされるようにしてもよい。

【０１３０】

なお、上記の実施形態は本発明の好適な実施の一例であり、本発明の実施形態は、これに限定されるものではなく、本発明の要旨を逸脱しない範囲において種々変形して実施することが可能となる。

【０１３１】

【発明の効果】

以上説明したように、本発明によれば、電子データに係るユーザＩＤ、およびデータ種別などが示されているワークフロー情報と、アクセス権限情報のテンプレートと、を用いてアクセス権限情報を生成する。従って、電子データに係るユーザＩＤおよびデータ種別などの簡単な情報を入力するだけで、電子データに対する複数のユーザのアクセス権限情報を容易に生成することが可能となる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態における文書発行ワークフローシステムを示す第１の図である。

【図２】

本発明の第１の実施形態における作成者端末のワークフロー情報作成時の画面表示を示す図である。

【図３】

本発明の第１の実施形態におけるワークフロー情報の一例を示す図である。

【図４】

本発明の第１の実施形態におけるＩＤが付与されたワークフロー情報を示す図である。

【図５】

本発明の第１の実施形態における文書発行ワークフローシステムを示す第２の図である。

【図６】

本発明の第１の実施形態におけるＡＣＬテンプレートを示す図である。

【図７】

本発明の第１の実施形態におけるＡＣＬの一例を示す図である。

【図８】

本発明の第１の実施形態におけるユーザ端末による印刷動作を示す図である。

【図９】

本発明の第１の実施形態におけるユーザ端末に設けられている表示装置の画面上に表示されるプリントダイアログを示す図である。

【図１０】

本発明の第２の実施形態におけるアクセス制御サーバの記録装置に登録されるセキュリティポリシーの一例を示す図である。

【図１１】

本発明の第２の実施形態におけるドキュメントのファイルタイプとセキュリティポリシーとの対応を示すマッピングテーブルを示す図である。

【符号の説明】

１　作成者端末

２　アクセス制御サーバ

３　承認者端末

４、４０２　ユーザ端末

１０　作成者クライアントプログラム

１１　ドキュメント

１２、１２ａ　ワークフロー情報

１３　保護ドキュメント

２０　ワークフロープログラム

２１　ドキュメント保護プログラム

２２　記録装置

２３　ＡＣＬテンプレートＤＢ

２４　ＡＣＬＤＢ

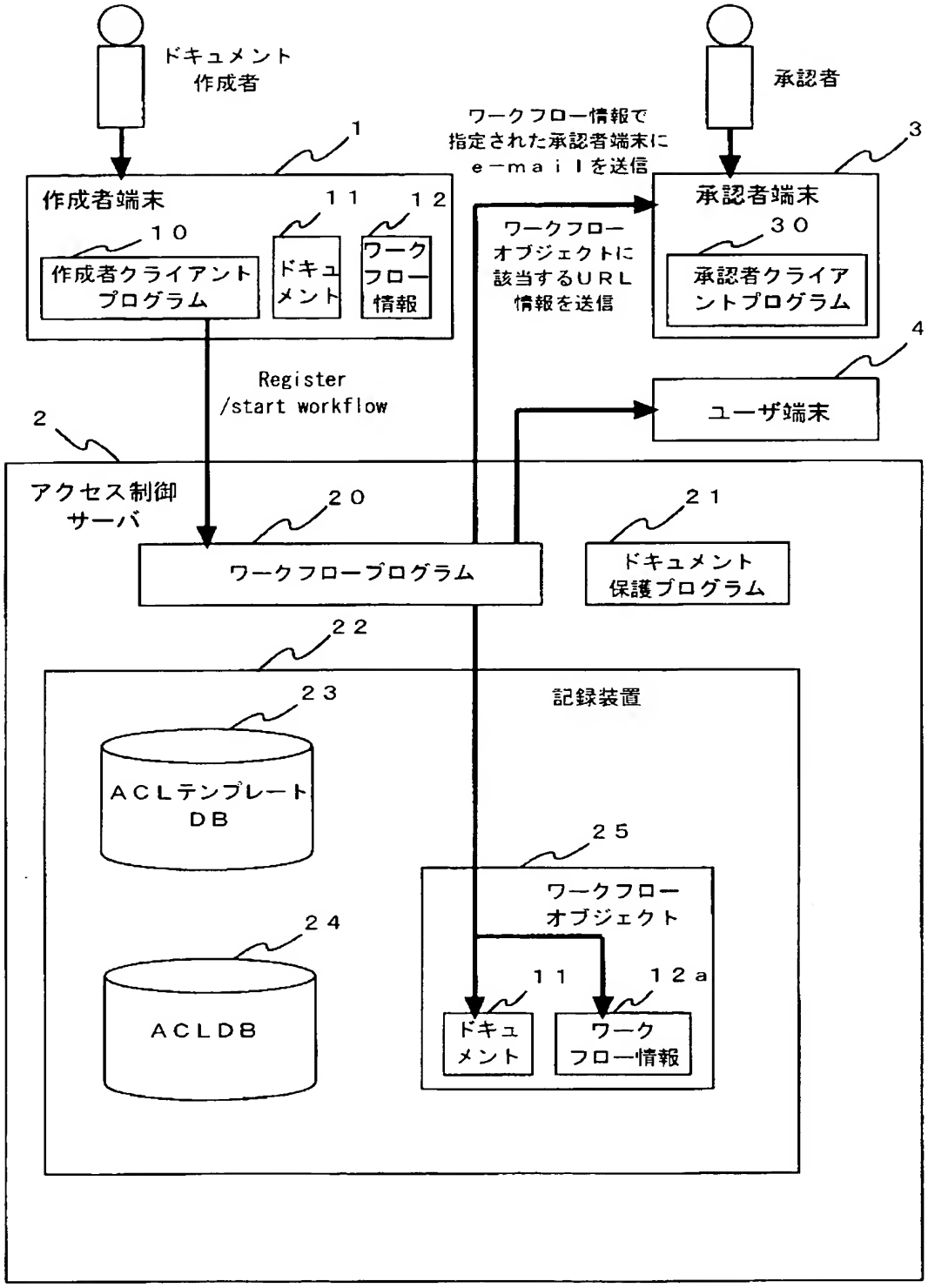
３０　承認者クライアントプログラム

４０３　プリンタ

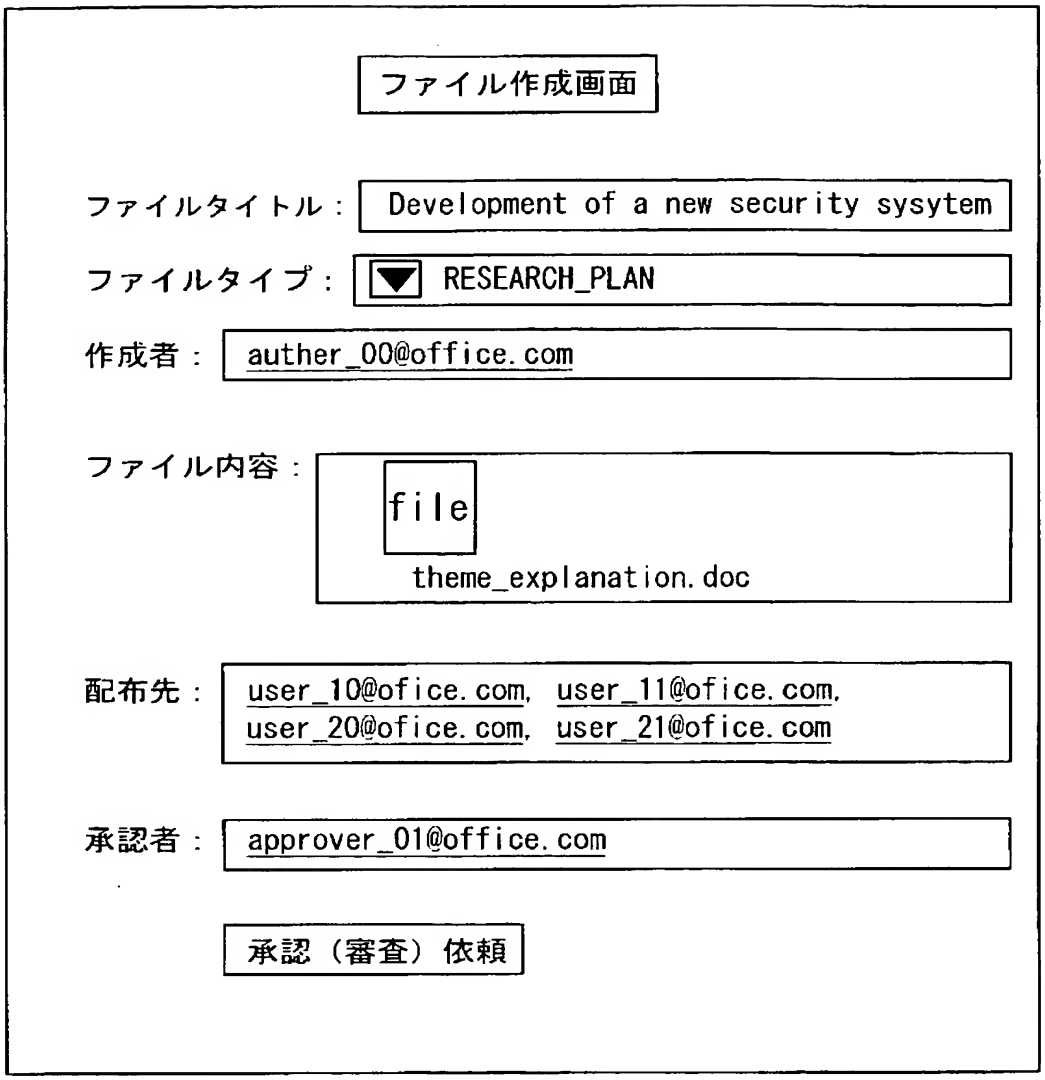
４２１　ドキュメント印刷プログラム

【書類名】　図面

【図１】


ドキュメント
作成者
承認者
ワークフロー情報で
指定された承認者端末に
ｅ－ｍａｉｌを送信
1
3
作成者端末
１１
１２
１０
作成者クライアント
プログラム
ドキュメント
ワークフロー情報
ワークフロー
オブジェクトに
該当するＵＲＬ
情報を送信
承認者端末
３０
承認者クライアントプログラム
4
Register
/start workflow
ユーザ端末
2
アクセス制御
サーバ
２０
２１
ワークフロープログラム
ドキュメント
保護プログラム
２２
２３
記録装置
ＡＣＬテンプレート
ＤＢ
２５
ワークフロー
オブジェクト
２４
１１
１２ａ
ＡＣＬＤＢ
ドキュメント
ワークフロー情報

【図２】


ファイル作成画面
ファイルタイトル：
Development of a new security sysytem
ファイルタイプ：
RESEARCH_PLAN
作成者：
auther_00@office.com
ファイル内容：
file
theme_explanation.doc
配布先：
user_10@ofice.com, user_11@ofice.com,
user_20@ofice.com, user_21@ofice.com
承認者：
approver_01@office.com
承認（審査）依頼

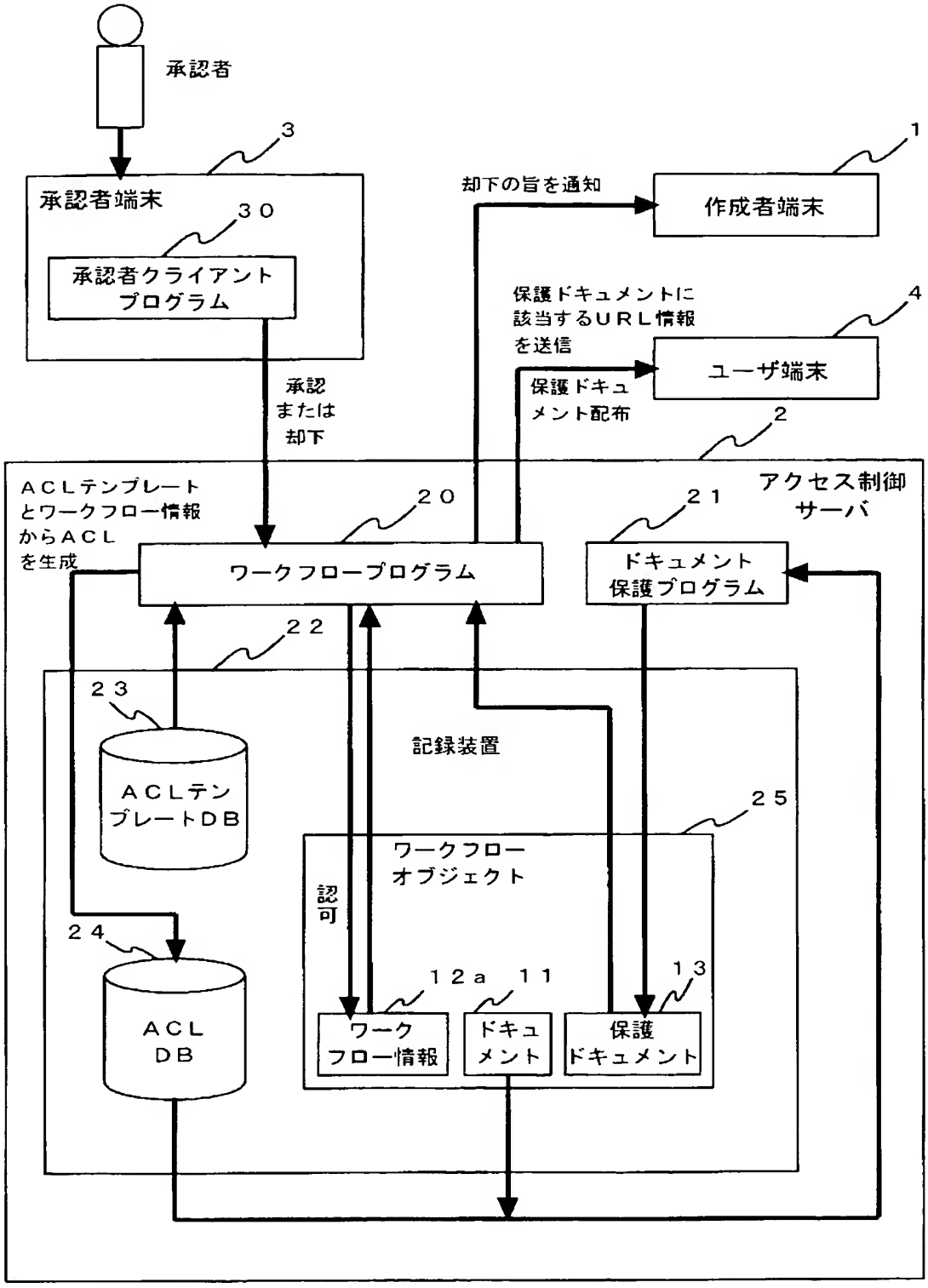
【図３】

ファイル名	Development of a new security system
ファイルタイプ	RESEACH__PLAN
作成者	author__00@office.com
承認者	approver__01@office.com
ファイル内容	theme__explanation.doc
配布先	user__10@office.com user__11@office.com user__20@office.com user__21@office.com

【図４】

```
<?xml version="1.0"encording="UTF-8"?>
<workflow_info>
        <id>011237835</id>
        <title>Development of a new security sysytem</title>
        <doc_type>RESEARCH_PLAN</doc_type>
        <status>wait_for_approval</status>
        <author>autor_00@office.com</author>
        <approver>approver_01@office.com</approver>
        <distribute_to>user_10@office.com</distribute_to>
        <distribute_to>user_10@office.com</distribute_to>
        <distribute_to>user_10@office.com</distribute_to>
        <distribute_to>user_10@office.com</distribute_to>
</workflow_info>
```

【図５】


承認者
3
承認者端末
30
承認者クライアント
プログラム
承認
または
却下
却下の旨を通知
1
作成者端末
保護ドキュメントに
該当するＵＲＬ情報
を送信
4
ユーザ端末
保護ドキュ
メント配布
2
アクセス制御
サーバ
ＡＣＬテンプレート
とワークフロー情報
からＡＣＬ
を生成
20
ワークフロープログラム
21
ドキュメント
保護プログラム
22
23
ＡＣＬテン
プレートＤＢ
記録装置
25
ワークフロー
オブジェクト
認可
24
ＡＣＬ
ＤＢ
12a
11
13
ワーク
フロー情報
ドキュ
メント
保護
ドキュメント

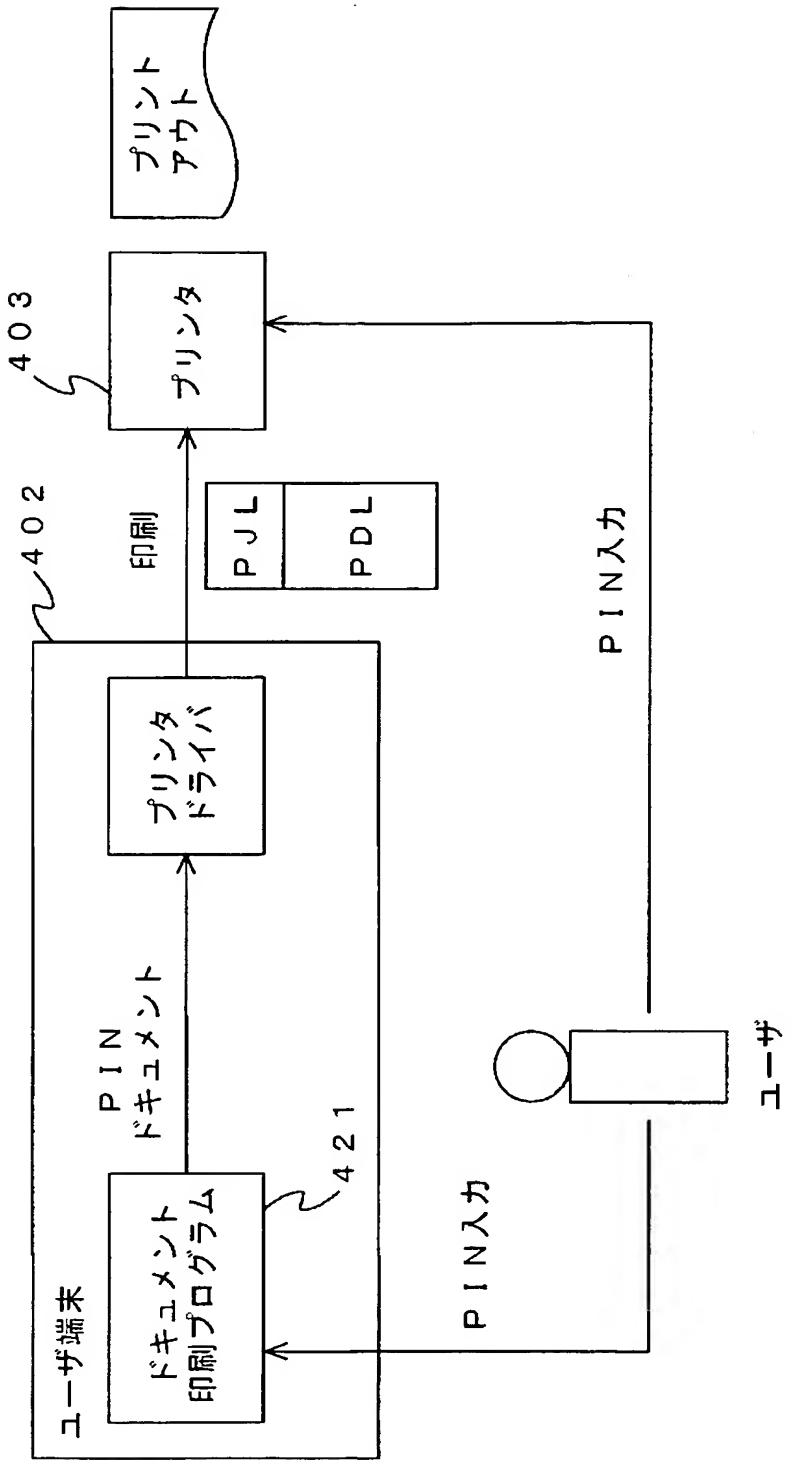
【図６】

User type	Access type	Permission	Requirements
author	Read	Allowed	–
	Write	Denied	–
	Print	Allowed	PAC(Private Access)
	Hardcopy	Allowed	–
approver	Read	Allowed	–
	Write	Denied	–
	Print	Allowed	PAC(Private Access)
	Hardcopy	Allowed	–
distribute_to	Read	Allowed	–
	Write	Denied	–
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Pattern)
			EBC(Embedding Barcord)
	Hardcopy	Allowed	RAD(Record Audit Data)

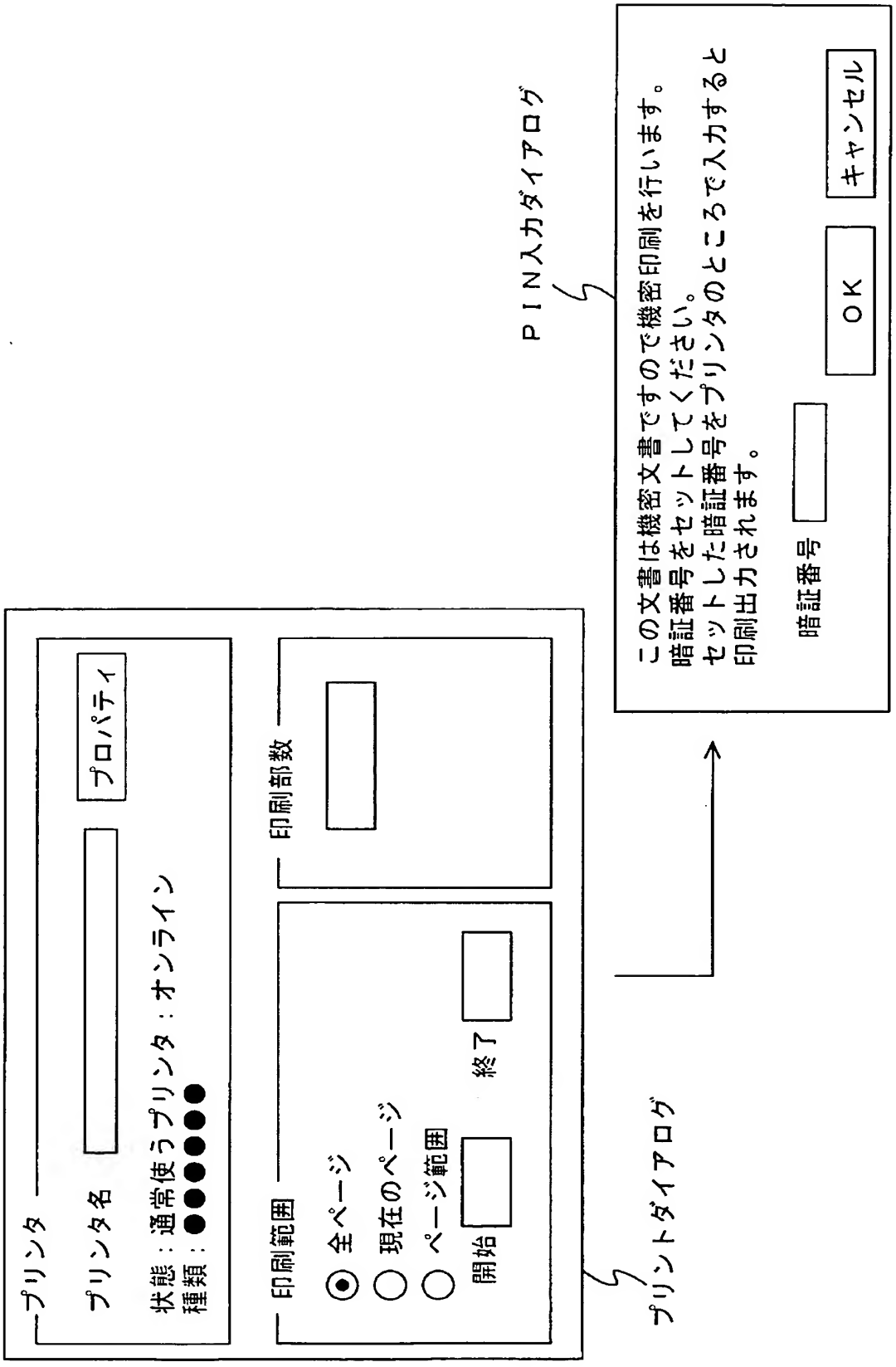
【図７】

User type	Access type	Permission	Requirements
author_00@office.com	Read	Allowed	–
	Write	Denied	–
	Print	Allowed	PAC(Private Access)
	Hardcopy	Allowed	–
approver_01@offide.com	Read	Allowed	–
	Write	Denied	–
	Print	Allowed	PAC(Private Access)
	Hardcopy	Allowed	–
user_10@office.com	Read	Allowed	–
	Write	Denied	–
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Pattern)
			EBC(Embedding Barcord)
	Hardcopy	Allowed	RAD(Record Audit Data)
user_11@office.com	Read	Allowed	–
	Write	Denied	–
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Pattern)
			EBC(Embedding Barcord)
	Hardcopy	Allowed	RAD(Record Audit Data)
user_20@office.com	Read	Allowed	–
	Write	Denied	–
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Pattern)
			EBC(Embedding Barcord)
	Hardcopy	Allowed	RAD(Record Audit Data)
user_21@office.com	Read	Allowed	–
	Write	Denied	–
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Pattern)
			EBC(Embedding Barcord)
	Hardcopy	Allowed	RAD(Record Audit Data)

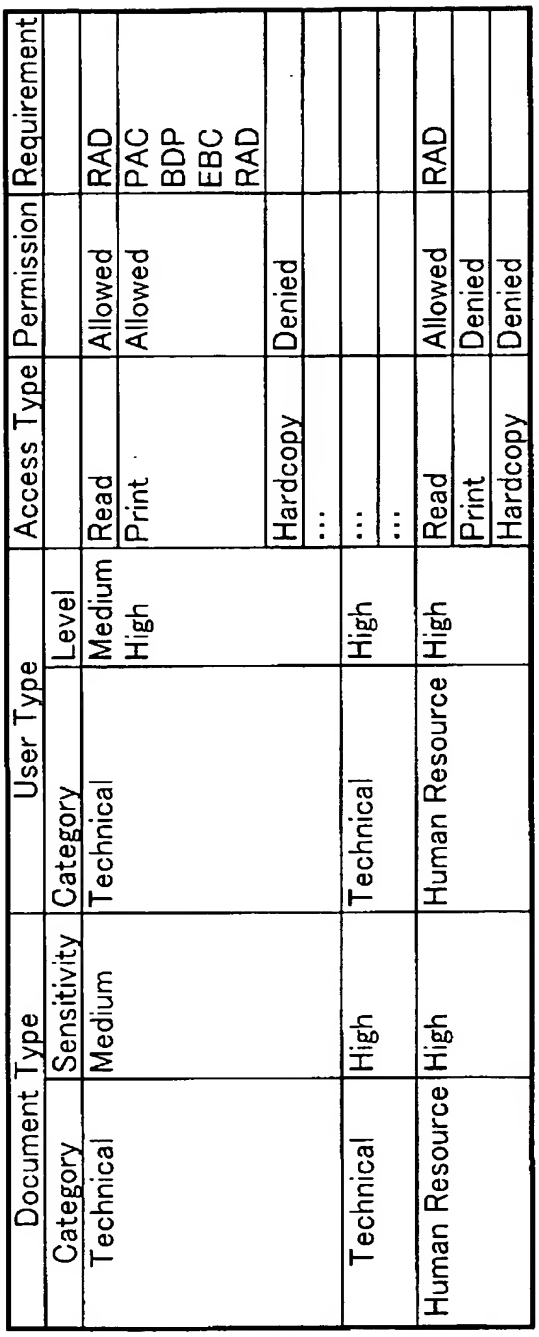
【図８】


プリントアウト
403
プリンタ
402
印刷
PJL
PDL
PIN入力
プリンタドライバ
PIN
ドキュメント
421
ドキュメント印刷プログラム
ユーザ端末
PIN入力
ユーザ

【図９】


プリンタ
プリンタ名
プロパティ
状態：通常使うプリンタ：オンライン
種類：●●●●●●
印刷範囲
全ページ
現在のページ
ページ範囲
開始
終了
印刷部数
プリントダイアログ
PIN入力ダイアログ
この文書は機密文書ですので機密印刷を行います。
暗証番号をセットしてください。
セットした暗証番号をプリンタのところで入力すると
印刷出力されます。
暗証番号
OK
キャンセル

【図１０】



Document Type		User Type		Access Type	Permission	Requirement
Category	Sensitivity	Category	Level			
Technical	Medium	Technical	Medium	Read	Allowed	RAD
			High	Print	Allowed	PAC BDP EBC RAD
				Hardcopy	Denied	
				...		
Technical	High	Technical	High	...		
				...		
Human Resource	High	Human Resource	High	Read	Allowed	RAD
				Print	Denied	
				Hardcopy	Denied	

【図１１】

Document type	Security attributes	
	Category	Sensitivity
RESEARCH_PLAN	Technical	Medium
GENERAL_CONTRACT	Contract	Basic
TOP_SECRET	General	High

【書類名】　要約書

【要約】

【課題】　電子データに対する利用権限を示すデータ（アクセス）を容易に生成し、その生成した利用権限を示すデータに基づいて電子データに対するアクセス制御を行うアクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体を提供する。

【解決手段】　アクセス制御サーバ２は、作成者端末１から受信したワークフロー情報１２にドキュメントＩＤを付加してワークフロー情報１２ａを生成する。アクセス制御サーバ２は、ワークフロー情報１２ａのファイルタイプに対応したＡＣＬテンプレートを抽出する。アクセス制御サーバ２は、抽出したＡＣＬテンプレートにワークフロー情報１２ａの作成者、承認者、ドキュメント配布先のユーザのユーザＩＤを挿入してＡＣＬを生成し、生成したＡＣＬに基づいてドキュメント１１に対するアクセス制御を行う。

【選択図】　図１

特願２００２－２９９６５８

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都大田区中馬込１丁目３番６号
氏　名　株式会社リコー

２．変更年月日　　２００２年　５月１７日
［変更理由］　住所変更
住　所　東京都大田区中馬込１丁目３番６号
氏　名　株式会社リコー